### **Prowler**

**Prowler**, AWS (Amazon Web Services) ortamları üzerinde güvenlik denetimleri yapan açık kaynaklı bir denetim aracıdır. Asıl amacı, bir AWS hesabında yanlış yapılandırılmış hizmetleri ve güvenlik açıklarını tespit etmektir. AWS'in en iyi güvenlik uygulamalarına (best practices) göre hesabınızı denetler ve uyumluluk raporları sunar. Ayrıca PCI-DSS, GDPR, HIPAA, ISO 27001 ve benzeri regülasyonlara göre kontrol profilleri de içerir.

Prowler; IAM, S3, EC2, CloudTrail, KMS, Lambda gibi AWS servislerinin yapılandırmalarını kontrol eder. Örneğin herkese açık S3 bucket’ları, şifresiz çalışan veritabanları ya da eksik CloudTrail log ayarları gibi riskleri otomatik olarak ortaya çıkarır.

### Prowler ne yapar?

AWS ortamında çalışan yüzlerce bileşen olabilir ve her birinin güvenlik ayarları ayrı ayrı kontrol edilmelidir. Prowler, bu kontrolleri otomatikleştirerek hem zamandan tasarruf sağlar hem de olası açıklara karşı sizi uyarır. Örneğin:

* S3 bucket’lar herkese açık mı?
* IAM kullanıcılarının MFA (Multi-Factor Authentication) aktif mi?
* CloudTrail tüm bölgelerde etkin mi?
* Güvenlik gruplarında 0.0.0.0/0 açık port var mı?
* EC2 makineleri şifrelenmiş disk mi kullanıyor?

Bu gibi soruları Prowler sizin yerinize sorar ve test eder.

### **Prowler kurulumu**

Prowler'ı çalıştırmak için AWS CLI'nin yüklü ve yapılandırılmış olması gerekir. Daha sonra aşağıdaki komutla kurulabilir:

* git clone https://github.com/prowler-cloud/prowler
* cd prowler

### Örnek kullanım

Tüm kontrolleri çalıştırmak için:

* ./prowler

Sadece belirli bir uyumluluk profiline göre (örneğin CIS AWS Foundations Benchmark) tarama yapmak isterseniz:

* ./prowler -g cislevel1

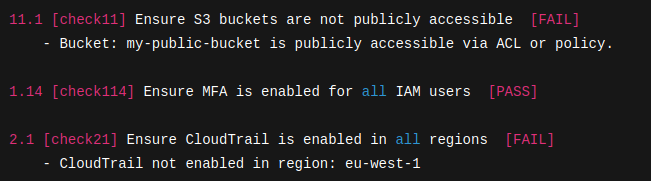
Yalnızca belirli bir servis üzerinde denetim yapmak için örnek:./prowler -c check11

* ./prowler -c check11

Bu komut yalnızca check11 isimli kontrolü (örneğin "S3 public access") çalıştırır.

**Çıktı örneği**

Tarama sonucunda Prowler detaylı bir rapor sunar. Örnek:



Bu örnekte:

* S3 bucket yanlış yapılandırılmış ve erişime açık.
* IAM kullanıcılarında MFA düzgün şekilde ayarlanmış.
* CloudTrail bazı bölgelerde devre dışı.

### Sık kullanılan parametreler

* -r <region>  
  Belirli bir bölgeye göre denetim yapar.  
  Örnek: ./prowler -r us-east-1
* -g <group>  
  Belirli bir kontrol grubunu çalıştırır (örneğin: cislevel1, gdpr, hipaa).  
  Örnek: ./prowler -g gdpr
* -c <control\_id>  
  Tekil kontrol çalıştırır.  
  Örnek: ./prowler -c check73
* -M <mode>  
  Çıktı formatını belirtir.  
  Desteklenenler: csv, json, html, json-asff  
  Örnek: ./prowler -M html
* -S  
  Sessiz mod. Daha az çıktı verir.
* -A  
  Tüm AWS servis bölgelerini (region) denetler